Insights into the cybersecurity challenges of Australia's lifeblood, SMBs

A Mimecast cybersecurity, privacy and risk leaders roundtable

SPONSORED BY

mimecast®

InnovationAus.com
PUBLIC POLICY AND BUSINESS INNOVATION

Attendees

Corrie McLeod
InnovationAus.com

Garrett O'Hara
Mimecast

Daniel McDermott
Mimecast

Melissa Lacey
Point River Networks

Annabel Reid
FifthDomain

Matt Wilcox
FifthDomain

Trent Dolphin
SentinelOne

Brandon King
ACSC

Jane Trewin
Box Hill Institute

Simon Richards
Small Business Ombudsman's Office

Prescott Pym
Deloitte

Louise McGrath
The Australian Industry Group

Tom McMahon
Tech Council of Australia

Introduction

Small to medium businesses (SMBs) are the backbone of the Australian economy, comprising 95 percent of all businesses in this country, and yet they also represent a significant cyber risk to the economy due to their lack of resources, support and knowledge in this area.

There is considerable time and energy spent by larger organisations and government to ensure they are securing their businesses and customers, and they still grapple with the complexity of the ever-evolving situation that is cybersecurity, so it's no wonder SMBs have fallen behind on this front.

InnovationAus.com, with the support of cybersecurity provider Mimecast, wanted to understand the issues affecting this large portion of Australian businesses, bringing together stakeholders from various sectors.

The aim of the discussion was to explore the particular challenges SMBs face ensuring adequate cybersecurity and strong cyber resilience, and to canvas some possible initiatives that could help them become more secure and resilient.

The overwhelming response from the closed-door discussion was that if cyber resilience for Australia as a whole is a priority, then there's a need to address the specific challenges for SMBs to ensure their cyber resilience is on par with larger organisations.

Just as healthcare has been addressed through a holistic approach, cybersecurity needs wholesale private and public sector support to ensure the right protection and support is given to the lifeblood of Australia's economy – SMBs. What can government do to make it affordable and effective – like Medicare? Afterall, the cyber health of these businesses will have a flow on effect to the rest of the country. So, isn't it vital the business of cybersecurity becomes everyone's business? Will people not sit up and listen until the true extend of the damage to the nation can be put into financial terms and the loss of productivity?

This issues paper summarises the discussion that took place at the *Cybersecurity, Privacy and Risk Leaders Roundtable Luncheon*.

The increasing importance of achieving these outcomes was explored in the context of the importance of SMBs to the Australian economy, the growing digital nature of SMBs, and new legislation to protect critical infrastructure that embraces a much larger range of businesses than the legislation it replaces.

The current situation and exposure of SMBs

In 2020, The Australian Cybersecurity Centre published the results of its survey of small businesses—those with less than 200 employees. Sixty two percent of respondents said they had experienced a cybersecurity incident and while 80 percent rated cybersecurity as 'important to very important', almost half reported spending less than $500 annually on cybersecurity. With data showing businesses start to outsource their cybersecurity support once annual turnover reaches $250,000, it appears financial capacity plays a large factor in cybersecurity spend. 97% of Aussie sole traders, for example, adopt a DIY approach.

Almost half of SMBs rated their understanding of cybersecurity as 'average' or 'below average' and admitted to having poor cybersecurity practices.

The ACSC survey also found SMBs greatly underestimated the impacts of a cybersecurity breach: 90 percent estimated they would recover from a cyber incident 'immediately' or 'within a few days', regardless of whether they had previously experienced a cyber incident.

The report identified barriers to good cybersecurity.

- Cybersecurity must compete for time and other resources with multiple other demands;
- Business owners fail to identify weaknesses in security practices and know they are struggling, but do not know where to begin.

The ACSC concluded: "Businesses need to better plan for and respond to cyber incidents … to better understand the risk and impact of a cyber incident and to not underestimate their recovery period from a cyber incident."

Data from the survey informed the contents of a series of ACSC guides to help SMBs with cybersecurity. However, in the ensuing two years the cyber threat has increased significantly, aided in part by the rise in communications usage resulting from COVID-induced remote working, and by the increasing digital nature of SMBs.

The ACSC reported a 15 percent increase in ransomware attacks between FY21 and FY22 and a survey undertaken by Avast found ransomware attacks, globally, increased 24 percent from Q1 to Q2 2022, with "cyber criminals increasingly targeting smaller organisations to encrypt crucial business data and disrupt operations."

SMBs cannot meet these cybersecurity challenges alone. What is needed are some co-ordinated initiatives from government, industry bodies, suppliers of cybersecurity products and services and higher education. Participants in the roundtable discussed the cybersecurity challenges faced by SMBs and canvassed a number of options to help them become more cyber secure and resilient.

State of readiness: defining SMBs' cybersecurity posture

In the context of cybersecurity, there needs to be awareness about the sensitivity of data being stored by a business versus its size. A hair salon, for example, may hold sensitive financial information regardless of its size or the number of employees, making it a target for cybercriminals. The importance of cybersecurity therefore needs to be determined by the data the business holds, the nature of the business and the requirements of other organisations in whose supply chains the business participates.

However, roundtable participants pointed out that many small businesses would hold personal data and likely be unaware of the legislated requirements to protect it, and the consequences of failing to do so.

"There is an issue that many small businesses collect personal information often without realising the significance of it, the risks that come with it both for them and for the people to whom it refers."

Protection measures incur costs, as does the loss of personal data, but this cost often falls on those whose data was exfiltrated. An analogy was drawn with legislation designed to prevent pollution. Absent effectively enforced legislation, the cost is born by the community, not the polluter. Effective regulation puts the cost on the polluter. Unless there are mechanisms to ensure SMBs protect customer data, the community bears the cost when personal data is exfiltrated. This prompted the question: "How can SMBs be incentivised, or constrained, to protect the personal data they hold?"

The roundtable identified two other significant cybersecurity pressures on SMBs: expanded critical infrastructure legislation and supply chains.

Delegates agreed that any change is likely to come through both incentives and consequences. The new critical infrastructure legislation is clearly a very big 'stick', but not one that can be used to beat every small business. One approach that could be very effective is large organisations at the head of supply chains requiring their small business suppliers to demonstrate adequate cybersecurity and cyber resilience.

Understanding the SMB ecosystem

There was much discussion around the many challenges a SMB faces trying to maintain cybersecurity and cyber resilience: lack of resources and expertise and the many demands of running a small business that leave little time to focus on issues not seen as core to the business. It was acknowledged that these challenges will remain and therefore most small businesses are never going to have significant in-house cybersecurity expertise. So whatever solutions are developed, they will have to recognise and work with this reality.

So, any solutions must also recognise and leverage the current means by which SMBs gain advice on cybersecurity: from their supplies of essential products and services.

Suppliers of products and services with an IT component, such as accountancy, payroll and telecommunications services, have trusted relationships with their SMB clients and the expertise to offer advice on cybersecurity and offer cybersecurity measures.

More and more businesses rely on the experts around them for guidance. If there is to be a wholesale change in cyber resilience, then the ability of these advisors needs to be a key focus. They need to be a clearly defined and engaged part of the solution. Cybersecurity may not be front of mind for small business owners, so it will fall to these advisors, as they are relied on heavily.

Even though much cybersecurity information is available on government and other websites (for example the ACSC guides mentioned above) many SMBs cannot devote the time and effort to finding, digesting and acting on it, and must lean on external experts or platforms to help.

"If you're an organisation that employs less than 20, people, you're lucky if you have some IT support, let alone cyber support. That's just the reality, and it's not going to change. If we're waiting around for a system where every small business is thinking about cyber, first and foremost, it's just not going to happen."

SMB cyber resilience through a socio-economic lens

It was pointed out that there are clear links between business health and cybersecurity 'health'. A business that is well run and thriving is far more likely to devote management time and money to cybersecurity and resilience than one living hand to mouth and struggling to make salaries every week.

Parallels were drawn with individual prosperity and dedication to physical and mental health. People on higher incomes are likely to eat healthier and exercise more, but society as a whole bears the costs resulting from the poorer health of low-income people. Similarly, society as a whole bears the costs resulting from SMBs' inadequate cybersecurity. When a company closes as the result of a cyber attack, people are thrown out of work. When a payment is diverted using a carefully crafted and timed fake email, it is the payer not the payee that bears the loss.

"These are small businesses. What is the bite-sized chunks, we can give them? What is the low hanging fruit that we can give them that makes 70 or 80 percent of a difference to their business model, but they can do in a short timeframe?"

Reframing cyber resilience through a productivity lens

It's an oft-repeated statement that SMBs are the backbone of the Australian economy. They represent more than 95 percent of all businesses, employ about 45 percent of all Australians and account for approximately 35 percent of economic output.

SMBs today are much more integrated into the digital economy than in the past. Therefore, the economy-wide importance of their cybersecurity and resilience has greatly increased. The isolation requirements of COVID-19 that led to a surge in remote working and online collaboration were only one contributing factor.

The Productivity Commission has noted a huge shift away from manufacturing towards professional services. Many of these services are delivered by small businesses and delivered completely online. It was suggested that the economic importance of small businesses' online activities, and hence of cybersecurity, could be used to mount a powerful argument for a government initiative of some kind aimed at improving SMBs' cybersecurity and resilience.

"Many people have very sophisticated online presences and have built their entire business online, but are they taking a cyber journey alongside that?"

Procurement and partnership drive resilience

It was suggested that a requirement to demonstrate at least some commitment to cybersecurity and resilience by SMBs vying for government business could help boost their cybersecurity. One suggestion was that implementation of the ACSC's Essential Eight cybersecurity requirements could be one yardstick by which SMBs' commitment could be judged.

Parallels were drawn with the US where the DoD requires small suppliers to meet minimal standards to prove they can be trusted with sensitive data.

With larger businesses now needing to ensure cybersecurity within their supply chains is airtight, it would be in the interest of SMBs aspiring to be involved in government procurement or partnerships with more mature businesses to do the same.

"We're seeing larger businesses worry more about their supply chains and invest more in their smaller supply chain partners."

Education and skills as a ‘Trojan Horse’ for cyber resilience

It was suggested there should perhaps be a course for SMBs or other source of information that provides a foundation level of understanding about cybersecurity and cyber resilience, but it is questionable, given the pressures and priorities most SMBs face, how widely it would be taken up.

Perhaps cybersecurity education needs to begin before the talent pipeline joins a small business. It was suggested cybersecurity could be part and parcel of vocational training, ensuring workers are taking the knowledge into a business with them.

There is no doubt that the digital literacy of the Australian population is increasing. School leavers today have been using digital technologies throughout their school years and have a level of understanding far greater than many older small business owners. Also, because almost every discipline today has a digital component, training in it can, and should, have a digital and cybersecurity component. People who go through training and into SMBs take with them an understanding of digital technology and cyber issues that will hopefully inform their employer and lead to an improvement in their cyber posture.

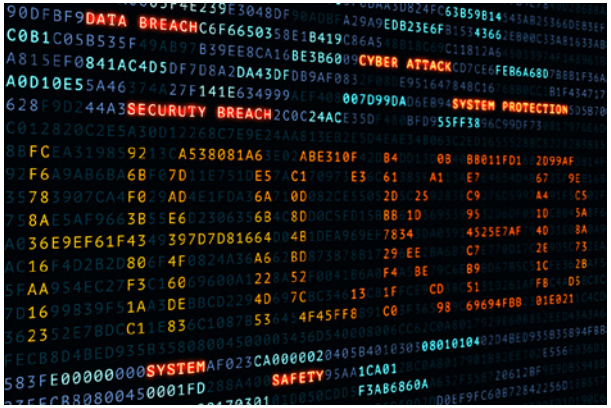
“In every discipline we deliver training in now we put a form of cyber training into it so students go back to their industry, to their employer, and say: ‘we should be doing this’.”

Getting the message across

It was agreed that 'burning platforms'—very specific pain messages that relay a sense of serious urgency—have their place in boosting SMBs' cyber resilience, and parallels were drawn with a highly effective road safety campaign in Victoria that contained horrifying graphic imagery.

It was also agreed that there are plenty of parallel horror stories in cyber without any specific campaign to promote them: stories of companies devastated by ransomware or embarrassed by massive leaks of personal information. Openness in sharing these real-world examples of the impact to SMBs would be highly impactful going forward.

However, it was suggested that good news stories might be more effective in spurring SMBs to take action rather than constant scare campaigns which can cause desensitisation and businesses to switch off. The strides and leaps taken in cybersecurity need to be highlighted via best use cases so that businesses know the hurdles are not insurmountable.



It was also suggested more specific messages that would get an SMB to take notice and act upon would need to come from an organisation seen as authoritative, such as a bank, and if these were to be effective in spurring SMBs to boost their cyber posture, the means for them to do so are readily available.

Public health and safety are analogous to cyber resilience

Public health and public safety are issues that merit, and receive, many specific programs, policies and legislation. Many of these are designed to help those unable to cater effectively for their own health, through lack of education, awareness or financial resources.

"When we're talking about small medium businesses [and cybersecurity], it's almost like someone who is middle class, or lower middle class that does not have access to the medicines, the health care, the lifestyle of higher socioeconomic classes. Telling them they need to adopt the Essential Eight is like saying, 'just eat better, move more, exercise more'. That's the idea, but it gets in the way of life."

Given the role of small business in the economy and the potential for damage and disruption that compromised cybersecurity can produce, there was agreement that SMBs' cyber resilience is an issue of national importance, requiring national initiatives.

"Ultimately, if you want to appeal to government to do something on a scale, you have to tap into the place that cybersecurity plays in the overall economy. And you have to be convinced that the government doing something is actually going to be a better benefit to the economy than letting the market do something."

Parallels were drawn with the measures to build resilience against, and respond to, natural disasters. Affected communities must be engaged in the planning and preparation. Trusted advisors need to be involved and a sense of community created around the issue. The challenges also need to be broken down into digestible, actionable components so as not to overwhelm members of the affected community.

"Our office has also done a fair bit of work around natural disaster resilience in the last year. And I see some real parallels between the approach you take to natural disaster resilience in terms of getting people to plan and how you engage people to plan around natural disasters, and how you get people to engage and people to plan around cybersecurity."

It was also pointed out that resilience comes from community, not necessarily from authorities. Parallels were drawn with responses to the recent floods in Lismore where local networks were far more effective than higher authorities in determining priorities and in providing information and support in real time.

"Small businesses share information. They find it from people that trust in different networks. So how do you tap into that?"

Coordination and consistency will triumph

There was consensus that lifting the cybersecurity and resilience of Australia's SMBs will be extremely challenging, but necessary, and that a 'stick' approach: legislation, regulation requiring certain levels of cybersecurity and resilience from SMBs will not on its own be sufficient: it would simply be beyond the means of many to achieve compliance.

Therefore, the best way to lift the cybersecurity and resilience of Australia's SMBs is by a co-ordinated approach that draws on the resources and expertise of organisations that possess these: governments, security vendors, industry organisations. Also, that to be effective, any initiative must be sustained, holistic and co-ordinated. Participants identified some significant initiatives that individual large players could already take.

Since 2003, Mimecast has stopped bad things from happening to good organisations by enabling them to work protected. We empower more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organisations worldwide.

Daniel McDermott
Senior Marketing Director, Mimecast
+61 3 8375 9774
dmcdermott@mimecast.com

SPONSORED BY

mimecast®

InnovationAus.com
PUBLIC POLICY AND BUSINESS INNOVATION